


the later specific date of _____.



Judge's signature

Honorable John M. Bodenhausen, U.S. Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:

4:22 MJ 1021 JMB

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **derrrickatikpo@gmail.com** that is stored at premises owned, maintained, controlled, or operated by **Google LLC**, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The content of all communications sent to or from the account (including through Gmail, Google Hangouts (including videos), and otherwise), stored in draft form in the account, or otherwise associated with the account, including all message content, attachments, and header information;
- b. All address book, contact list, or similar information associated with the account;
- c. Full Google search history and Chrome browser history associated with the account;
- d. All Google Drive content;
- e. All bookmarks maintained by the account;
- f. All services used by the account;
- g. All subscriber and payment information, including full name, e-mail address (including any secondary or recovery email addresses), physical address (including city, state, and

zip code), date of birth, gender, hometown, occupation, telephone number, websites, screen names, user identification numbers, security questions and answers, registration IP address, payment history, and other personal identifiers;

h. All past and current usernames, account passwords, and names associated with the account;

i. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;

j. All YouTube data associated with the account;

k. All transactional records associated with the account, including any IP logs or other records of session times and durations;

l. Any information identifying the device or devices used to access the account, including a device serial number, a GUID or Global Unique Identifier, Android ID, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the account;

m. All activity logs for the account;

n. All photos and videos uploaded to the account, including in Google Drive and Google Photos;

o. All information associated with Google Plus, including the names of all Circles and the accounts grouped into them;

- p. All photos and videos uploaded by any user that have that user tagged in them;
- q. All location and maps information;
- r. All Google Voice information;
- s. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- t. All privacy settings and other account settings, including email addresses or other accounts that the account has blocked;
- u. Advertising and Device Data: All advertising data relating to the account, including, but not limited to, advertising cookies, information regarding unique advertising IDs associated with the user, any devices used to access the account, Android IDs, application IDs, UDIDs, payment information (including, but not limited to, full credit card numbers and expiration dates and PayPal accounts), ads clicked, and ads created;
- v. Linked Accounts: All accounts linked to the Target Account (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise);
- w. For accounts linked by cookie, the date(s) on which they shared a cookie;
- x. For accounts linked by SMS number, information regarding whether the numbers were verified; and
- y. Customer Correspondence: All records pertaining to communications between the Service Provider and any person regarding the user or the user's account with the Service Provider, including contacts with support services, records of actions taken, and investigative or user complaints concerning the subscriber; and

z. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 1028 (fraud and related activity in connection with identification documents and information), 1030 (fraud related to computers), and 1343 (wire fraud) (hereinafter referred to as "the subject offenses"), occurring from Records from August 1, 2020 to August 16, 2021, or relating to Derrick Atikpo including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence relating to fraud and related activity in connection with identification documents and information, fraud related to computers, and wire fraud;
- (b) Evidence relating to communications and connections with foreign governments, entities, and individuals, including evidence relating to the conversion of intellectual property and trade secrets for the economic benefit of a foreign government, foreign instrumentality, or foreign agent;
- (c) information indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime(s) under investigation and to the email account owner;

- (d) Evidence indicating the email account owner's state of mind as it relates to the crime(s) under investigation;
- (e) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any United States personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, analysts, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agents may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the United States and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **Google LLC**, and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **Google LLC**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **Google LLC**, and they were made by **Google LLC** as a regular practice; and

b. such records were generated by **Google LLC** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **Google LLC** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **Google LLC**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature